GeoPlatform

Security Control Responsibilities

UNITED STATES DEPARTMENT OF INTERIOR

Version 1.0

June 2019

GeoPlatform

Cloud Broker provides operations as a Platform as a Service of the Geospatial mission associated with A-16 and EO 12906. An analysis conducted on GeoPlatform Cloud Broker operations identified customer responsible controls, fully inheritable and hybrid. The operations based on DOI contract GIS Award and FCHS contract can change, and these controls receive an evaluation on an ongoing basis to ensure they meet the Federal requirements (A-130, DOI Policy & FedRAMP) and the mission of GeoPlatform. Customers are responsible for their solution, access, and data in concert with Confidentiality, Integrity and Availability. Onboarding with the Cloud Broker identifies the solution, implemented. The implementation can affect the security controls and implementation statements written in the customer-system security plan. All parties should have a Support Level Agreement (SLA) in place to accept their responsibilities and risk.

Customer Responsible Controls -- 142

Control IDs	Security Control Names
AU-6	Audit Review, Analysis, and Reporting
AU-6(1)	Process Integration
AU-7	Audit Reduction and Report Generation
AU-7(1)	Automatic Processing
CA-2	Security Assessments
CA-2(1)	Independent Assessors
CA-3	System Interconnections
CA-3(5)	Restrictions on External System Connections
CA-5	Plan of Action and Milestones
AC-1	Access Control Policy and Procedures
AC-11	Session Lock
AC-12	Session Termination
AC-14	Permitted Actions Without Identification or Authentication
AC-2	Account Management
AC-2(2)	Removal of Temporary / Emergency Accounts
AC-2(3)	Disable Inactive accounts
AC-2(4)	Automated Audit Actions
AC-20	Use of External Information Systems
AC-20(1)	Limits on Authorized Use
AC-21	Information Sharing
AC-22	Publicly Accessible Content
AC-3	Access Enforcement
AC-4	Information Flow Enforcement
AC-5	Separation of Duties
AC-6	Least Privilege
AC-6(1)	Authorize Access to Security Functions

Control IDs	Security Control Names
AC-6(10)	Prohibit Non-Privileged Users from Executing Privilege Functions
AC-6(2)	Non-Privilege Access for Non-Security Functions
AC-6(5)	Privilege Accounts
AC-6(9)	Auditing Use of Privileged Functions
AC-7	Unsuccessful Logon Attempts
AC-8	System Use Notification
AP-1	Authority to Collect
AP-2	Purpose Specification
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-8	Accounting of Disclosures
AT-2	Security Awareness Training
AT-2(2)	Insider Threat
AT-3	Role-Based Security Training
AT-4	Security Training Records
AU-1	Audit and Accountability Policy and Procedures
AU-3(1)	Additional Audit Information
CA-6	Security Authorization
CA-7	Continuous Monitoring
CA-7(1)	Independent Assessment
CA-9	Internal System Connections
CM-1	Configuration Management Policy and Procedures
CM-2(3)	Retention of Previous Configuration
CM-2(7)	Configure Systems, Components, or Devices For High-Risk Areas
CM-3(2)	Test / Validate / Document Changes
CM-4	Security Impact Analysis
CM-7	Least Functionality
CM-7(1)	Periodic Review
CM-7(2)	Prevent Program Execution
CM-7(4)	Unauthorized Software / Blacklisting
CM-8	Information System Component Inventory
CM-8(1)	Updates During Installation / Removals
CM-9	Configuration Management Plan
CM-10	Software Usage Restrictions
CM-11	User-Installed Software
CP-1	Contingency Planning Policy and Procedures
CP-10(2)	Transaction Recovery
CP-2	Contingency Plan
CP-2(1)	Coordinate With Related Plans
CP-2(8)	Identify Critical Assets

Control IDs	Security Control Names
CP-3	Contingency Training
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training and Research
IA-1	Identification and Authentication Policy and Procedures
IA-4	Identifier Management
IA-5	Authenticator Management
IA-5(1)	Password-Based Authentication
IA-5(3)	In-Person or Trusted Third-Party Registration
IA-5(11)	Hardware Token-Based Authentication
IA-6	Authenticator Feedback
IA-7	Cryptographic Module Authentication
IA-8	Identification and Authentication (Non-Organization Users)
IA-8(1)	Acceptance of PIV Credentials From Other Agencies
IA-8(2)	Acceptance of Third-Party Credentials
IA-8(3)	Use of FICAM - Approved Products
IA-8(4)	Use of FICAM Issued Profiles
IR-1	Incident Response Policy and Procedures
IR-2	Incident Response Training
IR-3	Incident Response Testing
IR-3(2)	Coordination with Related Plans
IR-4	Incident Handling
IR-4(1)	Automated Incident Handling Purpose
IR-5	Incident Monitoring
IR-6	Incident Reporting
IR-6(1)	Automated Reporting
IR-7	Incident Response Assistance
IR-7(1)	Automation Support for Availability of Information / Support
IR-8	Incident Response Plan
MA-1	System Maintenance Policy and Procedures
MA-5	Maintenance Personnel
MP-1	Media Protection Policy and Procedures
MP-2	Media Access
PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan
PL-2(3)	Plan / Coordinate with Other Organizational Entities
PL-4	Rules of Behavior
PL-8	Information Security Architecture
PS-3	Personnel Screening
PS-4	Personnel Termination
PS-5	Personnel Transfer

Control IDs	Security Control Names
PS-6	Access Agreements
PS-7	Third-Party Personnel Security
PS-8	Personnel Sanctions
RA-1	Risk Assessment Policy and Procedures
RA-2	Security Categorization
RA-3	Risk Assessment
SA-10	Developer Configuration Management
SA-11	Developer Security Testing and Evaluation
SA-3	System Development Lifecycle
SA-4	Acquisition Policy
SA-4(1)	Functional Properties of Security Controls
SA-4(2)	Design / Implementation Information for Security Controls
SA-4(9)	Functions / Ports / Protocols / Services in Use
SA-5	Information System Documentation
SA-8	Security Engineering Principles
SA-9	External Information System Services
SC-1	System and Communications Protection Policy and Procedures
SC-10	Network Disconnect
SC-15	Collaborative Computing Devices
SC-17	Public Key Infrastructure Certificates
SC-5	Denial of Service Protection
SC-8	Transmission Confidentiality and Integrity
SI-10	Information Input Validation
SI-11	Error Handling
SI-12	Information Handling and Retention
SI-16	Memory Protection
SI-2(2)	Automated Flaw Remediation Status
SI-3	Malicious Code Protection
SI-3(1)	Central Management
SI-3(2)	Automatic Updates
SI-4(2)	Automated Tools For Real-Time Analysis
SI-4(4)	Inbound and Outbound Communications Traffic
SI-5	Security Alerts, Advisories, and Directives
SI-7	Software, Firmware, and Information Integrity
SI-7(1)	Integrity Checks
SI-7(7)	Integration of Detection and Response

Full Inheritance - 62

The purpose of the CIS is to delineate the control responsibilities of CSPs and customer agencies. The following controls are externally inherited from the FedRAMP Boundary CSPs FedRAMP security package and consists of 62 security controls that are fully inheritable:

Control IDs	Security Control Names
AU-8	Time Stamps
AU-8(1)	Synchronization With Authoritative Time
AC-11(1)	Pattern-Hiding Displays
AC-17	Remote Access
AC-17(1)	Automated Monitoring / Control
AC-17(2)	Protection of Confidentiality / Integrity Using Encryption
AC-17(3)	Managed Access Control Points
AC-17(4)	Privileged Commands / Access
AC-2(1)	Automated System Account Management
AT-1	Security Awareness and Training Policy and Procedures
CM-5	Access Restrictions for Change
CM-8(5)	No Duplicate Accounting of Components
CP-2(3)	Resume Essential Missions / Business
CP-4	Contingency Plan Testing
CP-4(1)	Coordinate With Related Plans
CP-6	Alternate Storage Site
CP-6(1)	Separation from Primary Site
CP-6(3)	Accessibility
CP-7	Alternate Processing Site
CP-7(1)	Separation from Primary Site
CP-7(2)	Accessibility
CP-7(3)	Priority of Service
CP-8	Telecommunications
CP-8(1)	Priority of Service Provisions
CP-8(2)	Single Points of Failure
CP-9	Information System Backup
IA-2	Identification and Authentication (Organization Users)
IA-2(1)	Network Access to Privileged Accounts
IA-2(2)	Network Access to Non-Privileged Accounts
IA-2(3)	Local Access to Privileged Accounts
IA-2(8)	Network Access to Privilege Accounts - Replay Resistant
IA-2(11)	Remote Access - Separate Device
IA-2(12)	Acceptance of PIV Credentials
IA-3	Device Identification and Authentication

Control IDs	Security Control Names
MA-3(1)	Inspect Tools
MA-3(2)	Inspect Media
MA-4(2)	Document Nonlocal Maintenance
MA-6	Timely Maintenance
MP-5(4)	Cryptographic Protection
MP-5	Media Transport
MP-6	Media Sanitization
PL-4(1)	Social Media and Networking Restrictions
RA-5(1)	Update Tool Capability
RA-5(2)	Update by Frequency / Prior to New Scan / When Identified
RA-5(5)	Privilege Access
SA-1	System and Services Acquisition Policy and Procedures
SA-4(10)	Use of Approved PIV Protocols
SA-9(2)	Identification of Functions / Ports / Protocols / Services
SC-12	Cryptographic Key Establishment and Management
SC-13	Cryptographic Protection
SC-2	Application Partitioning
SC-20	Secure Name / Address Resolution Service (Authoritative Source)
SC-21	Secure Name / Address Resolution Service (Recursive or Caching Resolver)
SC-22	Architecture and Provisioning for Name / Address Resolution Service
SC-23	Session Authenticity
SC-28	Protection of Information At Rest
SC-39	Process Isolation
SC-4	Information in Shared Resources
SC-7(3)	Access Points
SC-7(4)	External Telecommunications Services
SC-7(5)	Deny By Default / Allow By Exception
SC-7(7)	Prevent Split Tunneling for Remote Devices

Hybrid Security Controls -- 33

The following 33 security controls are considered hybrid. As with any services received by an external entity, they must be analyzed and determine if they fit your needs. After an evaluation, it is determined that these security controls are hybrid. There is a written explanation that will appear in the System Security Plan for those controls listed below. ISSOs, SOs, and AOs should review them to ensure their implementation meets the risk tolerance of the agency, document the policy and implement the security requirement of the control.

Control IDs	Security Control Names
AU-4	Audit Storage Capacity
AU-5	Response to Audit Processing Failure
AU-6(3)	Correlate Audit Repositories
AU-9	Protection of Audit Information
AU-9(4)	Access by Subset of Privileged Users
AU-11	Audit Record Retention
AU-12	Audit Generation
AR-7	Privacy-Enhanced System Design and Development
AU-2	Audit Events
AU-2(3)	Reviews and Updates
AU-3	Content of Audit Records
CM-2	Baseline Configuration
CM-2(1)	Reviews and Updates
CM-3	Configuration Change Control
CM-6	Configuration Settings
CM-8(3)	Automated Unauthorized Component
CP-10	Information System Recovery and Reconstitution
CP-9(1)	Testing for Reliability / Integrity
MA-2	Controlled Maintenance
MA-3	Maintenance Tools
MA-4	Non-local Maintenance
MP-3	Media Marking
MP-4	Media Storage
PS-1	Personnel Security Policy and Procedures
PS-2	Position Risk Designation
RA-5	Vulnerability Scanning
SA-2	Allocation of Resources
SC-7	Boundary Protection
SC-8(1)	Cryptographic or Alternate Physical Protection
SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-4	Information System Monitoring

Control IDs	Security Control Names
SI-4(5)	System Generated Alerts